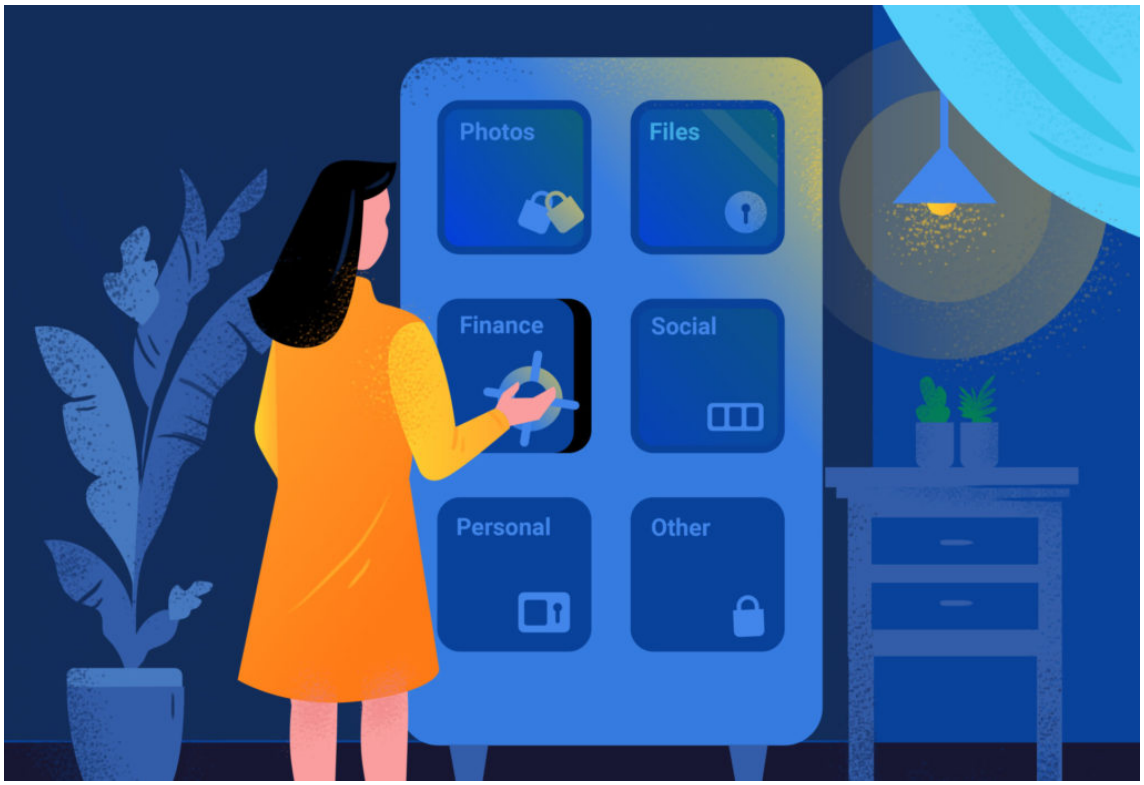
Videogames can save your digital future

Why you should play games at work

October 3, 2022



Security Measures by Afsal CMK [1]

The modern world becomes more and more digitized. Every day new forms of digital services, products and opportunities arise, while at the same time new forms of digital and physical attacks against these products arise as well. The key to all services is authentication of machines and humans. And while machines have moved forward at an unprecedented pace, humans are stuck at the most primitive mechanism of challenge and response, better known as passwords.

When looking through the variety of hacking, you will find highly innovative and sophisticated tutorials, write ups and much more in regards to authentication breaches. In reality, everyone, even you, probably knows at least one person that does not care about reusing the same password for every account, which can be guessed without being a cycbersecurity specialist. Whenever that person posts something on social media, such as place of living, birthdays, names of pets, friends or family, everyone can see it and that is all you need to crack a lot of passwords.

While this might not be very important for one's accounts on some blog's webpage, it becomes a harsh reality when looking at bank accounts, your personal Amazon account, your Bitcoin wallet and even more important your workplace password. Loosing your workplace password to a hacker can have serious consequences for the company you are working for and your future employment status at said company. Therefore you should not only secure your private accounts, but also your work accounts with

highly secure passwords.

While it can be difficult to create secure passwords, a new and innovative way to learn about reallife topics, called serious games, are here to support anyone who needs it. The topic of this blog post was nudged by G. Jayakrishnan et al. [2] and their USENIX paper *Passworld: A Serious Game to Promote Password Awareness and Diversity in an Enterprise*, which implemented a password based serious game to teach the company's employees about secure password creation.

1 Why your passwords are probably insecure and how to fix it

Determining the strength of your password is not trivial. Not only do different techniques with different results exist. But to make matter easier, there are a lot of available rules to choose from and the more you combine, the better the password will be. Classic rules include a minimum password length of 8, at least one number or one uppercase character and so on. But when looking at these basic rules, which people usually *have* to follow, because the password is not accepted otherwise, in Nordpass's Top 200 Most Common Password List of 2020 [3], 8 passwords in the top 50 are following these two basic rules. At this point, it has to be acknowledged that the databreaches from which these passwords were released

picture1	Million2	aaron431
password1	qqww1122	qwer123456
jacket025	1q2w3e4r	

Table 1: 8 Passwords from Nordpass in the top 50 [3] following 2 basic rules

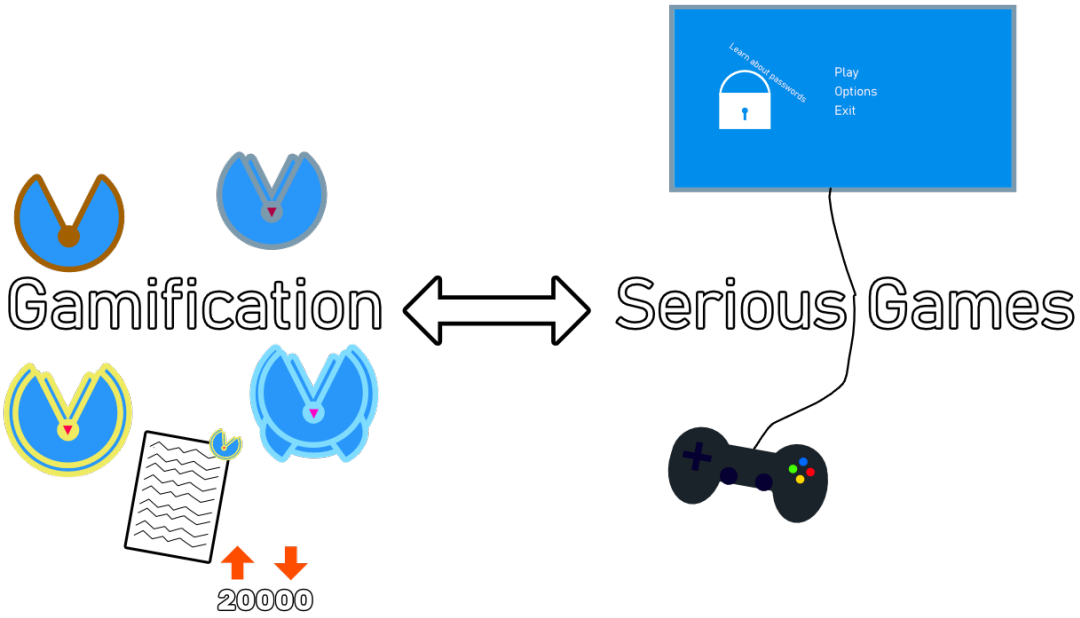
are not further named, and a bias towards less secure and less rule enforcing websites might very well be a viable reason for the state of the list. Nonetheless, the basic rules from before in addition with rules like at least one symbol, and at least one upper and one lower case, are not going to create more secure passwords inherently. But adding more complex and pattern destroying rules will eventually create strong and secure passphrases. Such rules can include no common words from the dictionary, no date formatted numbers, no increasing or decreasing sequence of characters and numbers, no keyboard patterns such as QWERTY, no repeated patterns of numbers and characters and many more. The goal is to add as much randomness as possible to it, increasing the difficulty to create heuristics about the password creation.

2 Applying the rules

While a large subset of the above rules, and the many other possibilities must be used during the password creation process, there are two fundamental problem left open to fix. One is the missing feedback on applying the rules. The other one is the mental capacity to remember a new password for each service, where each one should specifically be hard to guess and therefore hard to remember. In a private environment, remembering passwords is taken care of by many assisting programs, such as password managers, which should be used when using private accounts and systems. But when looking into business scenarios, it is usually not possible to install password managers on your work PC. Therefore it is very important to create long and strong passwords that at the same time are easy to remember. Every person has to find a way to remember those passwords, for example using additional techniques during the creation process, or starting with an easy to remember password and then applying all the required rules to it step by step. But the problem of remembering a large number of passwords is another problem and is not discussed any further.

In order to create feedback for applied rules and learn about new rules, a safe and secure playground is the best opportunity to test things out. That is the point where serious games come into role. A

serious game is a game, of any sort, which teaches the players about a certain topic while playing the game. The major difference of serious games to the more well known phrase of *Gamification* is clearly the way of application. Gamification refers to the integration of game like mechanics into real applications. Such mechanics often include badges, ranks, highscores and similar into existing services.



Difference in Gamification and Serious Games

Serious games on the other hand are complete games, which have the dedicated purpose to teach about a topic. Such a game is a safe place where the player does not have to fear any reallife repercussions if something is done wrong. Especially in the context of security, this is highly critical, as testing on live systems should never be done as it will endanger it. Additionally, games are often more fun and socially enjoyable than seminars and webinars. Learning this way can lead to higher participation and, in the long term, to better learning results. Serious games come in form of singleplayer or multiplayer games. Singleplayer games offer the great opportunity to be distributed as videogames to more players than classic board games (see section 3). This holds true especially in the current Covid-19 pandemic, which sees a huge increase in remote work setups, due to the tight workplace restrictions in many countries. In combination with the increase of video game traffic during the pandemic [4], more people than ever have played video games at least once. Inside a company the game can either be installed by the system administrators on each device or provided as an intranet online game. That is exactly what the paper of Jayakrishnan et al. [2] did with their serious game Passworld. It was provided as a company internal web game which could be played by any member of the company to learn about password creation rules. Many different rules were explained and tests before and after the playing were conducted to assess the impact of the game on the players. The basic game mechanics consist of 2 levels where the player has to find password resources, which allow him to use more characters in their password. The password then has to be used to secure artifacts which must be found in the 2d sidescroller game, in order to complete it. When a password was entered by the user, different animals, which represent password heuristics, come along and attack the password. If their heuristic is not fulfilled they break the password and the player looses a life and has to try again. During the exploration these animals can be found and talked to in order to learn about their password heuristic.

The results of the experiment inside the company were very positive, like other studies the authors refer to in their work as well. Compared to the test conducted before playing the game, players improved

their application of password heuristics by up to 3 times. Some heuristics however are more difficult to incorporate and learn from a single playthrough, such as no repeated characters, no keyboard patterns or predictable placement of uppercase letters in words. Repeating the playthroughs and tests again could have resulted in better performances, but was not tested by the team. However according to the tracking data from the video game, a substantial amount of people played the game more than one time during the experiment period. The additional comments from the participants were overwhelmingly positive, with over 90% of players enjoying the game, indicating that they learned about passwords and found the game very educational.

3 More to play

One educational game is better than none. But unfortunately cyberattacks can happen in so many facets that one game cannot be enough to teach each and every safeguard that is required in today's world. Especially so called *Social Engineering* attacks are on the rise and often easier to execute than a completely technical exploitation. Such a Social Engineering attack is an attack that uses "[...] acquisition of information about computer systems by methods that deeply include non- technical means" [5]. Because this attack can be executed against all employees of a company with a system account, every employee has to be trained to be aware of this threat. In order to provide a good way of learning, multiple games for Social Engineering training exist. The security company Kaspersky offers a game called *Industrial Protection Simulation* [6], which showed great results in a study from Yonemura et al. [7]. Another game, which was developed at the Technical University Munich by Beckers et al. [5], was tested on teams set up of people from different company departments. Everyone in the team can bring in new expertise and knowledge about different domains inside the company in order to improve the playthrough and learning effects for each other.

These 3 examples show how games can lead the way to a safer and more educated future. The goal for the future must be to develop more serious games for cybersecurity and beyond. In almost all areas games can be applied to teach new concepts, reinforce learning results and allow people to learn at their own pace with enjoyment on the way.

References

[1] A. CMK, *SECURITY MEASURES*, 2019. [Online]. Available: https://cybervisuals.org/visual/security-measures/.

[2] G. C. Jayakrishnan, G. R. Sirigireddy, S. Vaddepalli, V. Banahatti, S. P. Lodha, and S. S. Pandit, "Passworld: A serious game to promote password awareness and diversity in an enterprise," *Proceedings of the 16th Symposium on Usable Privacy and Security, SOUPS 2020*, pp. 1–18, 2020.

[3] Nordpass, *Top 200 most commen passwords of the year 2020*. [Online]. Available: https://nordpass.com/most-common-passwords-list/.

[4] A. Feldmann, O. Gasser, F. Lichtblau, E. Pujol, I. Poese, C. Dietzel, D. Wagner, M. Wichtlhuber, J. Tapiador, N. Vallina-Rodriguez, O. Hohlfeld, and G. Smaragdakis, "Implications of the covid-19 pandemic on the internet traffic," in *Broadband Coverage in Germany; 15th ITG-Symposium*, 2021, pp. 1–5.

[5] K. Beckers and S. Pape, "A Serious Game for Eliciting Social Engineering Security Requirements," in *2016 IEEE 24th International Requirements Engineering Conference (RE)*, 2016, pp. 16–25. DOI: 10.1109/RE.2016.39.

[6] Kaspersky Lab, "Kaspersky Interactive Protection Simulation," 2018. [Online]. Available: https://media.kaspersky.com/en/business-security/enterprise/KL_SA_KIPS_overview_A4_Eng_web.pdf.

[7] K. Yonemura, J. Sato, Y. Takeichi, R. Komura, and K. Yajima, "Security Education Using Gamification Theory," in *2018 International Conference on Engineering, Applied Sciences, and Technology (ICEAST)*, Jul. 2018, pp. 1–4. DOI: 10.1109/ICEAST.2018.8434432.